Elephant Beetle - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Elephant Beetle

Names	Elephant Beetle *(Sygnia)* TG2003 *(Sygnia)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2020
Description	(Sygnia) For the past two years, Sygnia's Incident Response (IR) team has been tracking a financially motivated threat group targeting and infiltrating organizations from the finance and commerce sector in Latin America. The attack is relentless in its ingenious simplicity serving as an ideal tactic to hide in plain sight, without any need to develop exploits. Using an arsenal of over 80 unique tools & scripts, the group executes its attacks patiently over long periods of time, blending in with the target's environment and going completely undetected while it quietly liberates organizations of exorbitant amounts of money. We are dubbing this group – Elephant Beetle. Elephant Beetle seems to primarily focus on the Latin American market, but that doesn't mean that organizations that are not based there are safe. Sygnia's IR team discovered and responded to an incident at a U.S. based company with an operations branch in Latin America. As such, both regional and global organizations should be on their guard. The group is highly proficient with Java based attacks and, in many cases, target legacy Java applications running on Linux-based machines as the means for initial entry to the network. Not only that, the group even deploys their own complete Java Web Application on the victim machine to do their bidding while the machine also runs the intentional application. This report is a technical play-by-play of the Elephant Beetle attack as detected, observed and mitigated by Sygnia's IR team. Elephant Beetle resembles the group tracked by Mandiant as FIN13.
Observed	Sectors: Financial. Countries: Latin America.

Tools used	jsp File browser, JSPSPY, MiniWebCmdShell, reGeorg.
Information	<https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia- Elephant Beetle_Jan2022.pdf>

Last change to this card: 25 January 2022

Download this actor card in PDF or JSON format
